O modelo de maturidade no contexto da proteção e privacidade de dados pessoais

NÍVEL DE MATURIDADE / PROCESSO DE ADEQUAÇÃO	1 – INICIAL	2 - REPETÍVEL	3 - DEFINIDO	4 - GERENCIADO	5 - OTIMIZADO
Gestão de Adequação e Prática da Privacidade	Poucas práticas e técnicas são seguidas (*Ad-hoc*), como minimização na coleta de DP, informações de privacidade aos titulares, etc.	Documentos sobre a proteção e privacidade de dados como boas práticas, procedimentos e regras, são compartilhados e utilizados.	Políticas e documentações formais, normas e regulamentos aprovados são comunicados e seguidos.	Revisões de políticas e procedimentos são escalados e utilizados, bem como a atuação da área de compliance. Utilizam-se indicadores para aferição dos processos (erros, adequação, retorno, etc.)	Processos são geridos de forma proativa e incremental em sua melhoria, com todos os procedimentos, normas int. e ext. (ex.: ISO 27701) e políticas sendo atualizados em busca da plena eficiência e integração.
Gestão de Governança	Conhecimento especializado em proteção de dados é somente identificada de forma pontual (pelo Depto. Jurídico, por exemplo).	Existe alguém que responde pela gestão da proteção de dados à nível operacional, como resposta às requisições de titulares, criação de conteúdo, etc.	Existe formalmente a função do DPO, com a política, as responsabilidades e funções, bem como grupos e papéis relacionados à Proteção e Privacidade.	O DPO mantém atualizados periodicamente os outros papéis de gestão da organização, com medição e análise quantitativa.	Existe a alocação permanente de recursos para a gestão de segurança e privacidade, visando a melhoria continuada dos objetivos levantados pelo DPO. Avaliações e estimativas de GAP são constantemente monitoradas e melhoradas.
Gestão de Operações	As operações de tratamento de DP são identificadas pelos colaboradores, funções ou papéis que as realizam, de forma pontual e não sistemática.	O processo de tratamento de DP é gerido de forma centralizada, por exemplo, informado ao responsável.	Existe a manutenção do registro de atividades de tratamento de DP, em conformidade com a LGPD/GDPR.	A integridade dos registros é verificada regularmente e existe um aumento na sua qualificação. (Ex: link para o documento de origem, mapa do processo, etc.)	A base dos registros é utilizada de forma proativa para a monitoria, descoberta, planos de melhoria e demais ações qualitativas. Mapeamento de processos são revistos e melhorados rotineiramente.
Gestão de Conformidade Legal	As informações gerais do tratamento, bem como eventuais avisos de privacidade são apresentados aos titulares quando na coleta dos DP, seja em modo físico ou on-line.	As operações de tratamento possuem avaliação com base no interesse legítimo e também nas necessidades e direitos dos titulares. Ademais, a privacidade e proteção de dados pessoais é referenciada nos contratos e demais termos entre a organização e o titular.	As políticas de compliance junto aos fornecedores, parceiros, clientes e titulares estão estabelecidas e seguidas pela organização (Ex: Acordo de Processamento, Tratamento Internacional, não divulgação, etc.). Quando necessário, o DPIA é implementado pelos responsáveis.	A checagem de medidas de privacidade, políticas, regras e procedimentos são monitorados, avaliados e alterados rotineiramente. Existe o uso de métricas e indicadores para a condução e melhoria de processos e do DPIA, por exemplo.	Políticas by Default e by Design estão fortemente acopladas aos processos da organização, melhorando constantemente a qualidade e segurança de todos os processos e novos projetos. Existe o monitoramento e ajuste das partes integradas às políticas de Due Diligence e também às operações de tratamento em conformidade com a legislação vigente.
Gestão de Conscientização e Treinamento	Alguns colaboradores pontuais têm a noção da privacidade e proteção dos dados pessoais e o impacto que pode acarretar junto à organização.	Existem papéis e funções com regras claras e direcionadas sobre as atividades de tratamento (ex.: comunicar o DPO sobre questionamentos de titulares).	Treinamentos são geridos de forma a integrar todos os envolvidos na cadeia de tratamento.	Existem indicadores destinados a monitorar o nível de adesão de todos os envolvimentos nos tratamentos.	Reciclagem e filtros são aplicados aos envolvidos para uma condução melhorada em todos os processos de tratamento. Treinamentos de atualização também são rotineiramente efetuados.
Gestão de Direitos dos Titulares	Requisições de titulares são tratadas como eventos independentes e sem um processo definido.	Existem documentos e diretrizes sendo seguidos em resposta às solicitações e direitos dos titulares.	Existem procedimentos de resposta padrão, com o uso de sistemas integrados que possibilitam acompanhar e gerir as solicitações dos titulares.	As solicitações que não estão dentro de um escopo padrão, são comunicadas e resolvidas pelo DPO. Indicadores do exercício de direitos dos titulares são revistos e discutidos rotineiramente.	Melhorias são tomadas com base nos indicadores de desempenho e as comunicações e avisos aos titulares são efetuados de forma proativa e integral.
Gestão de Riscos da Segurança da Informação	Medidas pontuais e *Ad-hoc* são utilizadas pela organização que trabalha de forma responsiva em grande parte do tempo (Ex.: atualização, encerramento de contas de usuário, etc.)	Existem políticas básicas, como a PSI, por exemplo, balizando a organização nas práticas de segurança da informação (Ex: uso de mesa limpa, uso de dispositivos móveis, e-mail e internet, etc.)	A organização conta com a gestão básica dos riscos de segurança (mais documental do que efetiva) que está ligada às operações de tratamento de dados pessoais e a formulação de DPIAs.	Existe autonomia de efetivar as ações necessárias para mitigar e gerir os riscos levantados, bem como há monitoramento e controle de riscos residuais e aderência ao apetite de riscos da organização.	A gestão de risco é monitorada, integrada e revisada periodicamente, visando a melhoria de todas as operações e tarefas relacionadas e está ligada fortemente com a gestão da continuidade dos negócios, técnicas de resiliência e demais atividades proativas.
Gestão de Violação de Dados Pessoais	Os incidentes são tratados como eventualidades e muitas vezes não geridas proficientemente (com registro, controle, comunicação, etc.).	Existe a comunicação e registro centralizado para determinar as ações a serem seguidas, bem como, notificação aos Titulares e/ou Agência nos casos de alto risco (de acordo com legislação pertinente).	A organização utiliza políticas de gestão de violação de DP, com processos de acompanhamento, tratamento e mitigação, atualizando as partes envolvidas sobre o andamento das ações de resolução e mitigação dos efeitos negativos.	O monitoramento e controle proativos são características chave, baseados em indicadores anteriores para a manutenção e implantação de mecanismos de segurança que evitem eventos futuros.	Análises periódicas são realizadas para a melhoria de todos os processos que possam resultar em violação, integrando-se com procedimentos by Design e by Default. Existe o uso de sistemas e agentes de detecção proativos visando mitigar quaisquer incidentes de violação.

Dúvidas? Contate o DPO:
https://www.linkedin.com/in/adriano-dpo
Out/2021

Fontes de Referencia:

LGPD: Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htmL
GDPR: Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 - https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN
ICO – Information Commissioner's Office - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
ISO/IEC 27001:2013 - Information security management systems
ISO/IEC 27002:2013 - Code of practice for information security controls
ISO/IEC 27005:2019 - Information security risk management
ISO/IEC 27701:2019 - Security Techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management
ISO/IEC 31000:2018 - Risk management – Principles and guidelines
ISO/IEC 22301:2020 - Business Continuity Management Systems
ISO/IEC 29190:2015 - Information technology — Security techniques — Privacy capability assessment model
ISO/IEC 21827:2008 - Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)
https://www.gid.net.br (documentação do pacote Consultor)
https://pt.wikipedia.org/wiki/Capability_Maturity_Model
https://www.cnil.fr/fr/la-cnil-propose-une-autoevaluation-de-maturite-en-gestion-de-la-protection-des-donnees